

UK Online Fraud

A CPP white paper



June 2010

Contents

2

1.1 Foreword

1.2 Industry Facts

1.3 Research methodology

1.4 Key Findings

- A cybercrime victim every seven seconds in the UK
- 420,000 scam e-mails are sent every hour in the UK
- E-fraud costs on average £289 per victim
- Fraudulent online purchases dominant
- Computer viruses considered the most likely threat
- A small minority think they are vulnerable to online fraud via their mobile phone

1.5 Conclusion

1.6 Avoiding Card Fraud

1.6 Q&A

1.8 Further Information

1.9 About CPP



Introduction

1.1 Foreword

There is no doubt that technology and the economic situation have worked in partnership to change the face of fraud over the last few years.

The introduction of Europay-MasterCard-Visa (EMV) enabled cards in 2005 undoubtedly changed the way fraudsters worked and saw them shift card fraud to the internet. Although overall losses from card fraud fell in 2009, Chip and PIN is highlighted as the major factor behind an 11 per cent fall in fraud on lost and stolen cards – now at its lowest in two decades. Losses at UK retailers have also fallen by 67 per cent since 2004 and mail non-receipt fraud has fallen by 91 per cent since 2004.

The decrease in phone, internet and mail order shopping fraud classified as card-not-present fraud (CNP) has been attributed to the increased sophistication of fraud screening tools by retailers and banks, as well as the continuing growth in the use of MasterCard SecureCode and Verified by Visa. In 2009 CNP fraud decreased 19 per cent.

The growth of fraud has clearly been via online banking as fraudsters look to target consumers directly for their sensitive account information. This increase is largely due to criminals using more sophisticated methods to target online banking customers through malware, which targets customers' PCs, rather than the banks' systems which are much more difficult to penetrate. The prevalence of phishing has also been a major factor in the growth of online fraud and of phone banking fraud losses. The latter is a relatively new phenomenon whereby customers are tricked into disclosing security details through cold calling which criminals then use to commit fraud.

The recession has also played its part. The rise in account takeover and the growth of identity fraud has been the result of fraudsters attacking the consumer directly. Fraudsters, well aware of the reduction in the overall amount of lending taking place during 2009 and 2010, have been discouraged from attempting to commit application fraud – the use of lies and forged documents in an attempt to obtain products or services. The 25 per cent reduction in application fraud has meant they have turned their attentions to account takeover and identity fraud.

Account takeover typically happens when a fraudster hijacks an individual's account in order to 'takeover' and 'control it'. Account takeover has increased 250 per cent during the last two years and a major contributory reason for this is the prevalence of phishing e-mails. During 2009, identity fraud increased 35 per cent with over 85,000 people having their identities hijacked by fraudsters.

“

The prevalence of phishing has also been a major factor in the growth of online fraud

”

As credit becomes easier, the strength of the pound increases, and consumers become familiar with phishing attacks, it will be interesting to see fraud trends for the first half of 2010 when these are published in October by the UK Payments Association. In particular it will be interesting to see whether the reduction in CNP fraud was a temporary blip after years of significant increases or a sign of things to come. Equally, whether online banking fraud losses will plateau or continue to increase.

The results of the report show that UK consumers are nevertheless being bombarded with online scams and a significant proportion falling victim to the associated financial and damaging emotional and psychological residual effects.

1.2 Industry Facts

- 51,161 unique phishing attacks in 2009 in the UK – a 16 per cent increase on the 2008 figure (UK Cards Association March 2010)
- In 2009, the US had the most overall malicious activity measured by Symantec, with 19 per cent of the total
- The majority of brands used in phishing attacks in 2009 were in the financial services sector, accounting for 74 per cent (Symantec)
- Total UK payment fraud in 2009 was £440.3m (UK Cards Association March 2010)
- Online banking losses totalled £59.7m up 14 per cent on 2008 (UK Cards Association March 2010)
- 50 per cent of UK internet users engage in online banking (Electronic Payments International May 2010)
- 23 per cent increase in victims of identity fraud in the first quarter of 2010, with almost 27,000 victims (CIFAS – UK Fraud Prevention Service March 2010)
- According to the latest figures from the Office of National Statistics 37,400,000 UK adults have access to the internet
- People in the UK lose an estimated £3.5bn every year to mass market fraud (SOCA Serious organised Crime Agency June 2010)

1.3 Research Methodology

CPP commissioned research in April 2010 to establish how prevalent online attacks are in the UK. The research looked at how many consumers have ever fallen victim to online fraud and the financial costs to the individual. The aim was to quantify the level of risk consumers feel and the different ways they were targeted.

A representative sample of just over 2,000 UK adults was questioned by Research Now between 23 and 30 April 2010.

“
51,161
unique
phishing
attacks
in 2009
in the UK
”

1.4 Key Findings

A cybercrime victim every seven seconds in the UK.

According to the latest figures from the Office of National Statistics 37,400,000 UK adults have access to the internet. According to the research 26 per cent of consumers have fallen victim to online fraud. Of this figure 19 per cent have fallen victim once, five per cent twice and two or three per cent three or more times.

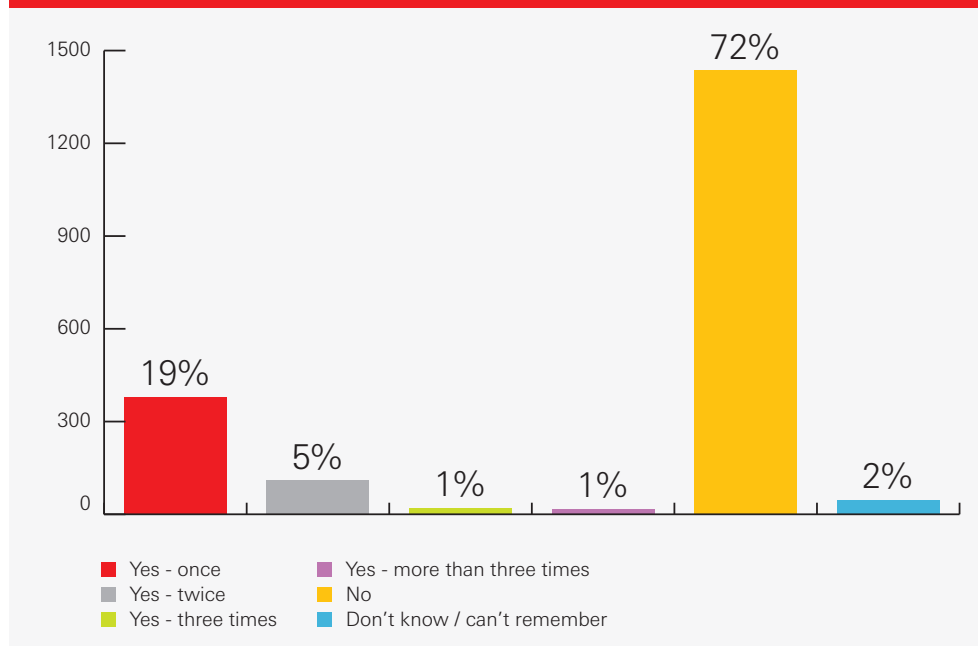
Those aged 25-34 (35%) and 35-44 (36%) are the most likely to claim to have been a victim, versus only 21 per cent of those aged 55-64.

Brighton claimed the highest number of online fraud victims (39%) versus Glasgow, Nottingham and Plymouth (22%).

48 per cent of these victims claimed to have fallen victim in the last 12 months. We can therefore estimate 4,667,520 online victims in the last year.

When asked how they realised they had fallen victim, 29 per cent said it was when they were contacted directly by their bank, 13 per cent when goods didn't arrive and they became suspicious and eight per cent when contacted by a website saying it had been hacked.

Q: Have you ever been a victim of online fraud?



“

3.7 billion
scam e-mails
over a
12-month
period,
equating to
420,661 scam
e-mails every
hour

”

420,000 scam e-mails are sent every hour in the UK.

75 per cent of consumers have received fraudulent e-mails in the past 12 months. Fake banking e-mails, commonly known as ‘phishing’, are the most common method used by criminals, with 55 per cent of those targeted receiving seemingly legitimate e-mail correspondence from high-street banks – usually to verify account details and security information.

Over half (52%) also received false lottery or competition prize draws, while a further one in two (47%) had received bogus e-mails from abroad saying they were entitled to money.

61 per cent of 35-44 year olds claim to receive phishing e-mails verses 50 per cent of 18-24 year olds. The relatively small variance across age groups highlights the manner in which criminals target millions of people in the hope of defrauding a small minority.

When we asked consumers how many of these e-mails they suspect to be fraudulent, the average number was 11 per month or 132 a year. With 37,400,000 UK adults using the internet and three quarters receiving fraudulent e-mails, we can estimate 3.7 billion scam e-mails over a 12-month period, equating to 420,671 scam e-mails every hour.

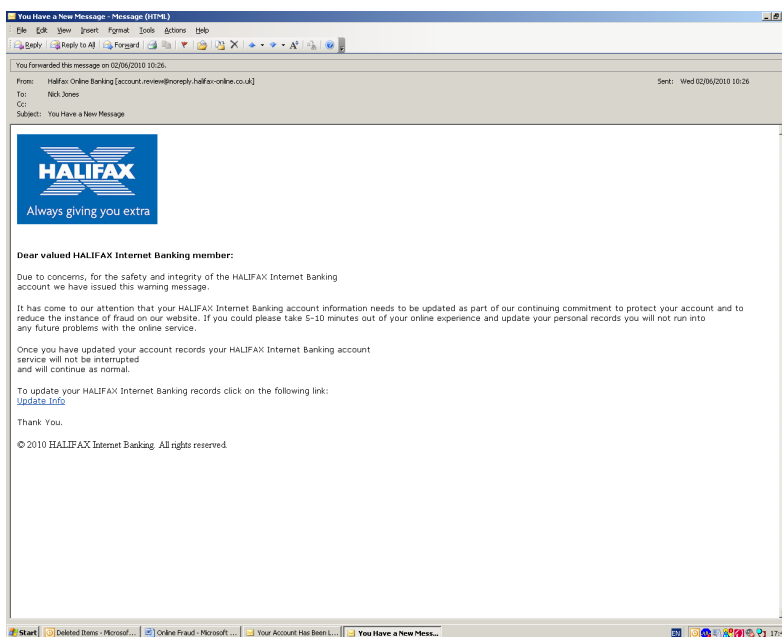
Men were more likely to report more fraudulent e-mails (12.72) verses women (8.96).

Residents in Belfast (13.67) reported the highest number of fraudulent e-mails followed by Brighton (12.44) and Birmingham (12.39). Residents in Newcastle reported the lowest frequency of fraudulent e-mails (8.04).

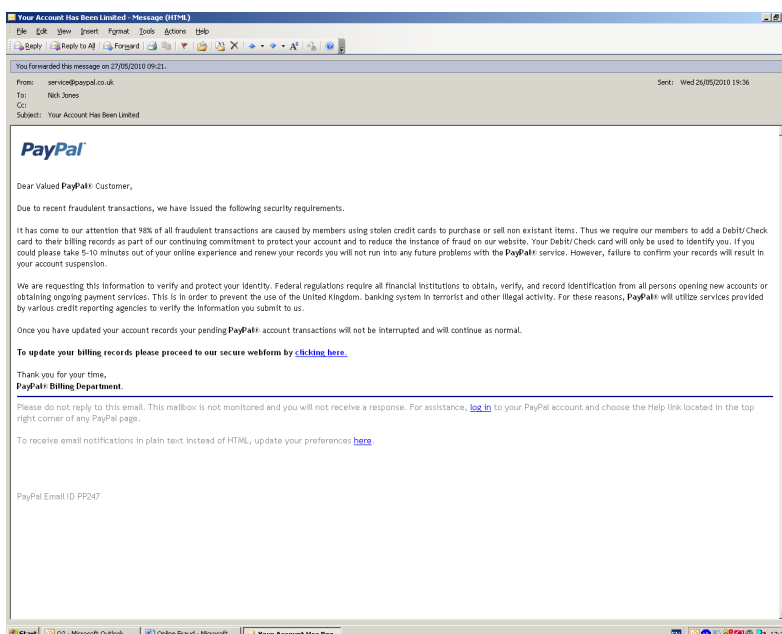
The credit crisis and subsequent banking crisis certainly gave fraudsters an excellent opportunity to increase their phishing attacks. As bank and building societies rapidly merged with one another they legitimately contacted their customers telling them about the changes. Fraudsters jumped on this opportunity to solicit personal and financial information. It will be interesting to see if the number of phishing attacks and financial losses to CNP and online banking decrease now this opportunity has passed.

As more and more consumers worldwide use the internet for shopping and organising their lives, fraud is increasingly likely to move online, and, according to Symantec, malware poses the greatest threat. In their latest report ‘Global Internet Security Threat Report’ April 2010, Symantec indicates that the number of worldwide malware samples increased 71 per cent in 2009 compared to 2008. Symantec put the popularity of this attack down to the fact of the increasing number of people using online banking. In the UK and France, penetration of online banking is 50 per cent, while in Canada the number rises to 60 per cent and in the US 80 per cent. Clearly there is a huge potential market for fraud.

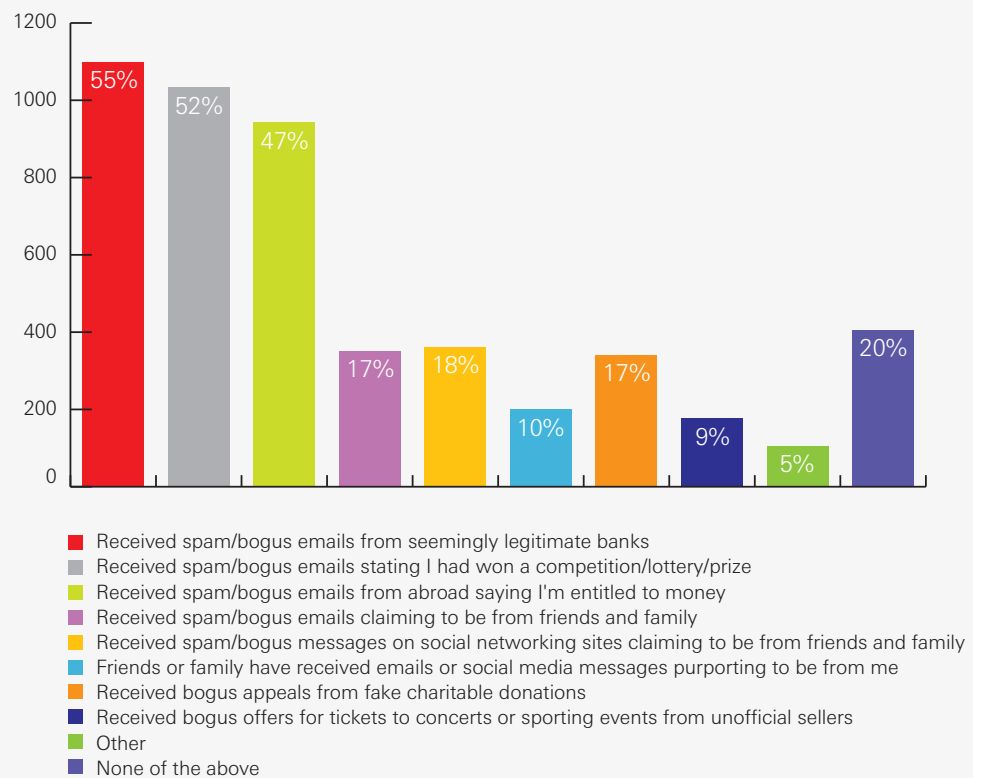
An example of a phishing e-mail asking for updated internet banking account information:



An example of a phishing e-mail asking for debit card details to reduce the incidence of fraud:



Q: Have you experienced any of the following in the past 12 months?



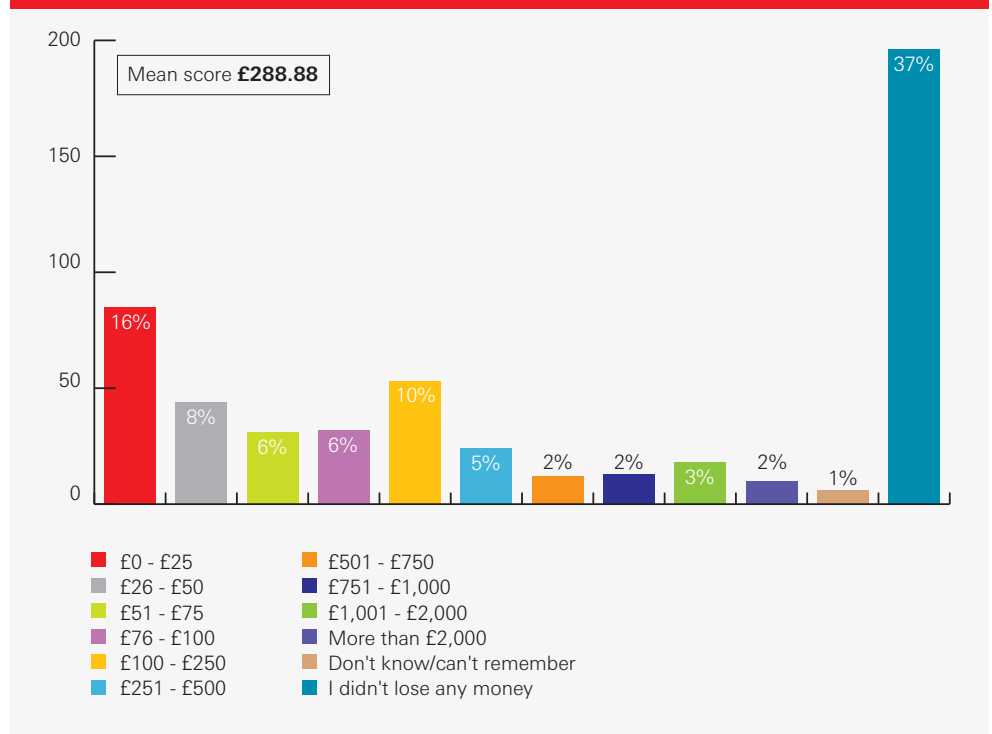
E-fraud costs on average £289 per victim.

26 per cent admit to falling victim to e-fraudsters and on average the financial loss was £289.

Men reported a slightly higher mean loss of £327.70 versus £246.54 for women. As you might expect, older people (65+) experienced greater losses (£462.93) as opposed to the losses experienced by younger people – £108.27 (18-24), £199.53 (25-34). This is no doubt influenced by the amount of available credit.

Regionally, consumers in Brighton reported the largest losses to online fraud (£690.23) followed by Liverpool (£512.86) and Birmingham (£360.95). Residents in Norwich reported the lowest losses (£65.56).

Q: In your most recent instance of online fraud, how much did you lose as a result of falling victim?



Fraudulent online purchases most common consequence.

The most common consequence of online fraud was when a consumer's debit or credit card details were used to make online purchases. This is consistent with the proliferation of phishing e-mails over the last 24 months and affected 41 per cent of victims.

Other common consequences included goods and tickets bought online but never arriving (15%), money being stolen directly from the victim's account (14%) and PC and laptops being infected with viruses (10%).

The rise in phishing attacks has contributed to the increased vulnerability of consumers. The table below charts the increase in the number of unique phishing attacks and the financial losses attributed to online banking fraud losses.

	2005	2006	2007	2008	2009	% change 2008-09
Online banking fraud losses (£m)	23.2	33.5	22.6	52.5	59.7	14
Number of phishing attacks	1,700	14,156	25,797	43,991	51,161	16

Source: UK Cards Association, March 2010

The increased losses attributed to online banking and other losses attributed to card-not-present (CNP) fraud is the result of Chip and PIN, which has driven fraud down at point-of-sale, but seen it migrate into new areas. Although Chip and PIN is defenceless against CNP fraud, online authentication solutions such as Verified by Visa and MasterCard SecureCode have helped drive losses down by 19% in 2009 (£266.4m), the first time this kind of fraud has recorded a year-on-year decrease.

Whilst there was little variance between gender, those aged 18-24 were more likely to buy tickets or goods online that didn't arrive (22%), have their social networking profile hijacked to send soliciting messages (15%) or be impersonated on social networking sites (9%) than older demographics. In contrast people above the age of 35 were far more likely to have their payment cards used for fraudulent transactions.

Elsewhere when asked where they think they are at risk, 46 per cent of people voiced concerned that their card details could be used to make illegal purchases online.

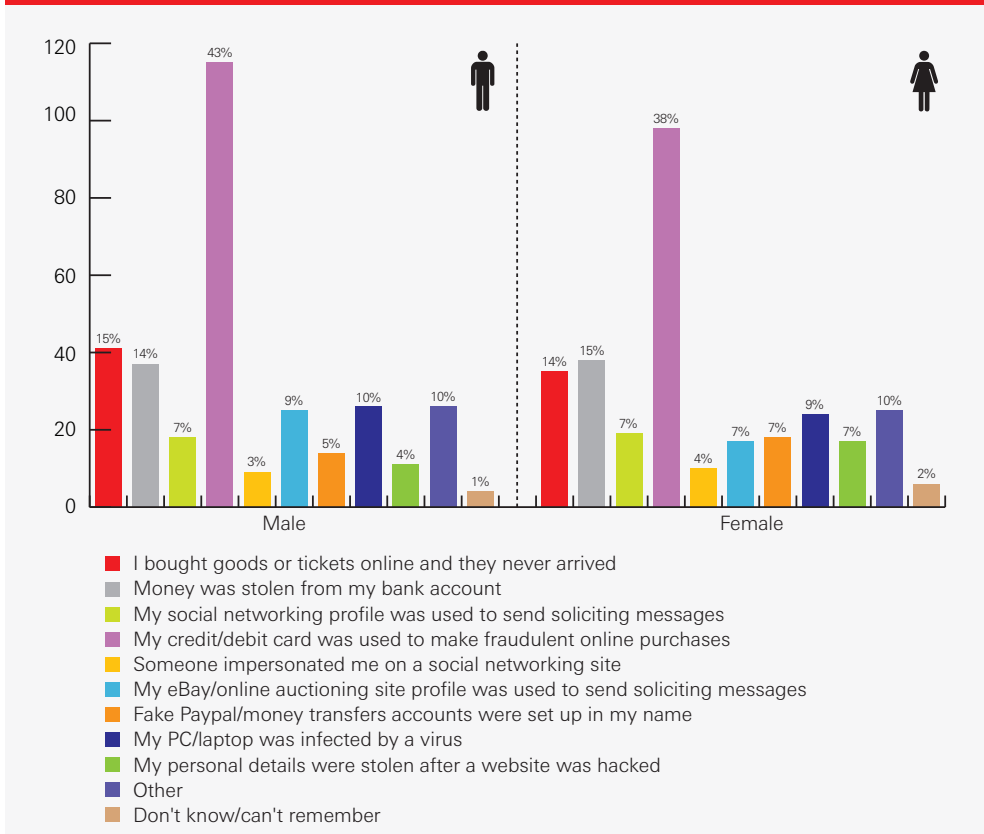
According to Cybersource's 2010 UK Online Fraud Report, on average merchants reject 4.6 per cent of online orders due to suspicion of fraud, a figure that has largely remained unchanged over the years.



46 per cent of people voiced concern that their card details could be used to make illegal purchases online



Q: Thinking about your most recent instance of online fraud, what happened as a result of you falling victim?



Computer viruses considered the most likely threat.

Despite 44 per cent of respondents saying they protect themselves with paid for anti-virus software, 34 per cent via anti-phishing tools and 77 per cent with active firewalls, 61 per cent of consumers think they are at most risk from computer viruses.

The perception of this risk is highest amongst those aged 18-24 and lowest aged 64+.

Elsewhere having personal information stolen online is considered a threat to financial security with half of people concerned. This has no doubt been made worst by the number of data breaches in the media. Specifically the NHS reported 305 data breaches to the Information Commissioner's Office (IOC) since November 2007. The figure for the NHS compares to 288 for the private sector, 132 for local Government and 18 for Central Government.

The fear of CNP fraud ranks third with 46 per cent concerned that their cards could be used to make illegal payment online with those aged 35-44 most concerned (52%)

As a result of the massive publicity attributed to social media and in particular the anxiety around default security settings, bogus e-mails through social networking sites, personal accounts hacked into and fraudsters following people are now high on the public's consciousness. As you might expect, it is those under the age of 34, but in particular 18-24 year olds, who report the greatest anxiety. 64 percent of those aged 18-24 are concerned about bogus messages and nearly 20 per cent are concerned about a fraudster following them on Twitter.

On Facebook, it has been widely reported that default settings are set to 'socialise' and are open for all to see. With over 170 security settings across multiple pages, it can be time consuming to lock these down and make access secure to friends only. A common social network scam involves fraudsters hacking an account, such as Facebook, Twitter or MySpace and then contact friends and family claiming they are in trouble and need money to be sent immediately to a specified address.

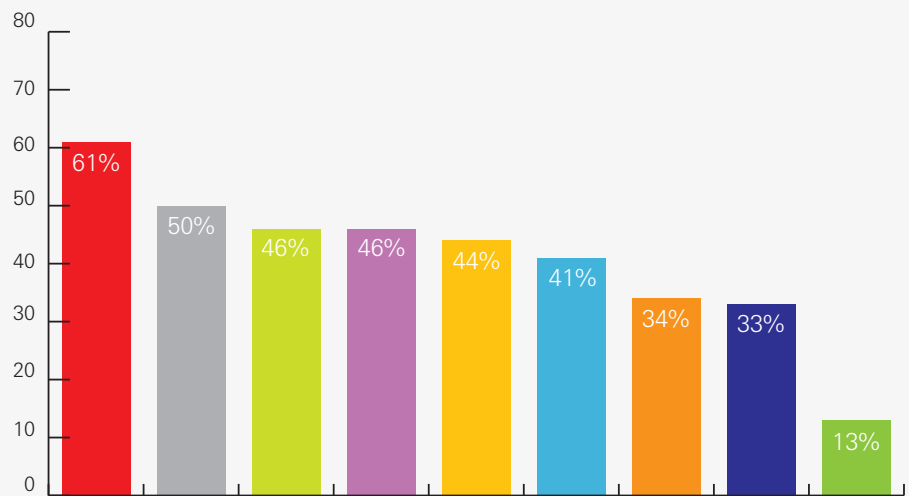
Residents in Belfast (72%), Glasgow (71%) and Brighton (69%) were the most concerned about computer viruses. When asked if they would be upgrading or purchasing anti-virus software/protection in the next 12 months, 56 per cent said they would, 23 per cent said they would not and 21 per cent did not know. Men (42%) were marginally more likely to upgrade their protection than women (37%) in order to stay one step ahead of the cybercriminals.

“

On Facebook,
default
settings are set
to 'socialise'
and are open
for all to see

”

Q: Do you think that you are at risk from the following?



- Being infected with a computer virus
- Having personal data stolen online
- Having my card details used to make illegal purchases online
- Having my e-mail account hacked into
- Receiving bogus e-mails through social networking sites
- Having my online passwords stolen and used fraudulently
- Having my social networking account hacked into
- Having my bank account hacked into
- Having a fraudster follow me on Twitter

A small minority think they are vulnerable to fraud via their mobile phone.

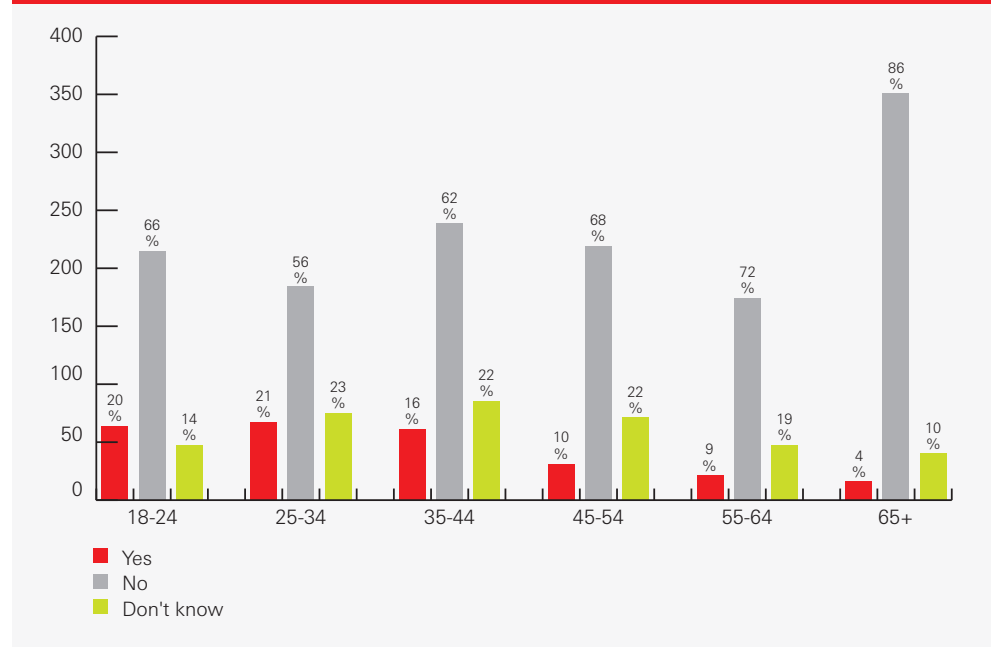
Looking to the future and the migration of contactless payments to mobile payments, our research shows us that a small minority is concerned about fraud via their mobile phone. In April 2010 Forrester Research said that one fifth of consumers surveyed did not believe mobile banking was safe¹, indicating that industry players have a long way to go before consumers are truly convinced about the security of mobile payment technologies.

According to Gartner Research² mobile payment users will reach 190 million in 2012, representing more than three per cent of mobile users worldwide. In Western Europe penetration is expected to rise from 0.9 per cent in 2009 to 2.5 per cent in 2012.

Elsewhere in March 2010 Pay Pal reported Pay Pal mobile transactions increased nearly six-fold over the last year, rising from \$25 million in 2008 to \$141 million in 2009.³

As expected, and no doubt consistent with the awareness/penetration of smart phones, it is those aged under 34 that are most aware of the fraud risk via the mobile. When asked if they have any software on their handset to reduce the risk of fraud only a very small minority (4%) said they do.

Q: Do you think you are at risk of falling victim to online fraud through your mobile?



“
Those aged under 34 that are most aware of the fraud risk via the mobile
”

1 Smart phones to drive European m-banking take-up' Forrester Research, April 2010
2 Dataquest Insight: Mobile Payment, 2007 – 2012, Gartner Research, 27 April 2009
3 PayPal launches new Send money app for iPhone, PayPal, 2010

“
The proliferation of scam e-mails has clearly reached epidemic levels
”

1.5 Conclusion

The proliferation of scam e-mails has clearly reached epidemic levels. According to our report more than 420,000 scam e-mails are sent every hour in the UK, with a victim every seven seconds. Overall a quarter of people claim to have fallen victim to some form of online fraud and the average victim is estimated to lose over £285 each.

The proliferation of e-mail scams is also complemented by fake websites. In May the IKEA, 'Gift Card Scam' defrauded 70,000 victims and the Serious Organised Crime Agency has publicly put the cost of mass market web scams at £3.5 billion every year. Online dating sites and gaming sites are becoming particular favourites of cyber criminals looking to mine personal information.

Fake banking e-mails are clearly the most common method used by criminals; with over half of those targeted receiving seemingly legitimate e-correspondence from high-street banks. Over half received false lottery or competition prize draws, while a further one in two was targeted by foreign cons such as the renowned 'Nigerian 419 advance free fraud scam'.

Fraudsters are also exploiting the popularity of social networking sites and current defaults in privacy settings to target victims. Nearly one fifth of consumers have received phoney Facebook messages claiming to be from friends of family – one very common scam is for fraudsters to hijack a social networking account and then contact friends and family claiming they are in trouble and need money to be sent immediately to a specified address.

It seems anyone can fall victim to online fraud. Tim Berners-Lee, creator of the worldwide web, became a victim after buying Christmas presents online, which failed to show up. Film star Salam Hayek had her Apple MobileMe account attacked and not even politicians are immune – Ed Milliband's Twitter account was infiltrated by hackers who posted details of a fictitious personal life.

Demographically younger consumers seem more at risk via social networking sites via hijacked accounts or buying goods and services online that fail to materialise. Older people tend to lose more money, probably because they have more funds deposited, and through their cards being used online. The perceived risk of fraudulent spending on payment cards was high across all respondents with nearly half fearing this was a real risk. The fear of computer viruses was also very prominent helping to encourage nearly half of consumers to upgrade or purchase anti-virus software in the next 12 months.

Looking towards the future of payments, a small minority think they could be vulnerable to fraud via their mobile phone and no doubt consistent with the penetration of smartphones, it tends to be those aged under 34 that are most aware of the risk of fraud via the handset.

Despite regional and differences amongst different age groups, the important point to remember is that online fraud can affect anyone. Consumers need to remain vigilant and not to respond or open any e-mails or visit any websites that they suspect to be fraudulent.

1.6 Avoiding Card Fraud

Michael Lynch is an identity fraud expert at CPP and offers the following advice to consumers to help protect them from identity fraud. Michael is responsible for the UK Identity Protection portfolio at CPPGroup Plc (CPP).

Michael has been with CPP for 14 years. His experience in financial services extends to customer service, new product and market development and affinity relationships.

During his time at CPP, Michael has helped bring to market one of the UK's market leading service, Identity Protection, which now protects over one million UK consumers from the consequences of this rapidly growing crime. In addition, Michael had used his expertise to create a commercial identity theft product aimed at protecting businesses of all sizes. He has also developed a strong understanding of consumer perception and reaction to identity theft and its consequences. In addition Michael has been responsible for breaking some major identity theft stories in the media, including the availability of fraudulent documents online, car cloning, junk mail and postal theft. Committed to forging industry co-operation to reduce the opportunities for identity theft he is leading the call for consumers to change their behaviour to counter what is becoming an increasingly sophisticated and intrusive crime.

Michael is media trained across print and broadcast and is available for media interviews on the issue of identity fraud.

1.7 Q&As

Q What is the headline story?

A More than 420,000 scam e-mails are sent every hour in the UK according to our research. This equates to 3.7bn scam e-mails over the last year. Worryingly, a lot of people are actually falling for these scams. More than a quarter of people say they have fallen victim to fake banking e-mails, fake prize draws and scams from abroad. The amounts that people are losing are not insignificant either. The average amount stolen by e-fraudsters is nearly £300 per person.

Q How did you calculate his hourly rate of scams?

A Our research shows that 75 per cent of Brits have received fraudulent e-mails or messages in the past year. It also shows that people have received at least 11 fraudulent e-mails per month which equates to 132 per year.

If you take these figures and multiply them by the number of adults that have access to the Internet in the UK (37.4 million) then it gives you over 3.7 billion scam e-mails received per year.

If you divide this by 365 you get the number of fraudulent e-mails per day, and if you divide this further by 24 you get the number of fraudulent e-mails per hour which equates to 422,671.

Q What were the main findings of the research?

A Our research shows that there is a victim of cybercrime every seven seconds in the UK, as people fall for phishing e-mails, fake competitions and scams from abroad. In fact more than a quarter of people in the UK have fallen victim to e-fraudsters, with the average person losing almost £300 each time.

Fake banking e-mails are the most common method used by criminals, closely followed by fake competitions and scams from abroad.

We also found that fraudsters are also exploiting the explosion of social networking sites to target victims. Nearly one fifth of Brits have received phoney Facebook messages claiming to be from friends or family – and one in 10 fear that fraudsters are using Twitter to follow them.

Q How did you calculate that there is a cybercrime victim every seven seconds?

A According to our research 26 per cent of Brits have fallen victim to online fraud and 48 per cent of these in the last 12 months. If you take this proportion of the population and multiply by the number of people that have access to the Internet you get 4,667,520 victims last year.

If you divide this by 365 this amounts to 12787 victims a day. If you divide this by 24 you get 532 victims an hour. If you divide this by 60 it works out as 8.88 victims a minute, which means one victim every seven seconds.

Q What is online fraud?

A Online fraud has many different guises. Typically, it refers to when someone tries to acquire your personal or financial information online to rack up illicit purchases, or run up debts in your name. It can take the form of sending fake or “phishing” e-mails to your e-mail address, hijacking e-mail accounts and social networking profiles to ask people for money, or using illicitly-gained card details to make purchases online.

Q How big is the problem?

A The sheer scale of the problem is breathtaking. Our research shows that there is a cybercrime victim every seven seconds in the UK, with more than 420,000 scam e-mails sent every hour.

What’s really concerning is that so many people are still falling victim – over one in four of us. We may be getting savvier with technology, but it seems that we are also becoming complacent with our personal and financial information online and putting ourselves at unnecessary risk.

Q What are the most common scams?

A Fake banking e-mails are the most common method used by criminals, where fraudsters imitate the logos and e-mail structures of real banks and ask you to enter your financial details. They can then be used to make illicit purchases in your name, or can be sold-on to fraud gangs abroad. It’s important to remember that your bank will never ask you to enter your financial details online, so if you receive e-mails like this, phone your bank immediately.

E-mails saying you’re entitled to money or have won a competition are also common, as is the growth in fraudulent messages sent via social networking profiles.

Q Surely people are aware of these scams now?

A While some scams, such as the “Nigerian 419 con” have become infamous in recent years, fraudsters are becoming ever-more sophisticated in their methods. Fake banking e-mails in particular have become almost indistinguishable from legitimate ones, with logos and company styles being imitated almost perfectly.

Q Who tends to be affected the most?

A It tends to be young adults who tend to be most affected, possibly due to the popularity of social networks among younger people, or that they are shopping online more. But it’s important to remember that online fraud can affect anyone. It’s important to remain vigilant and not to respond to or open any e-mail you suspect to be fraudulent.

Q Why are so many people falling victim?

A It could be for a number of reasons, from people being tricked by extremely accurate fake banking e-mails, to responding to fake messages on social networking sites which they think have come from their friends or family. It could even be a case of fraudsters hacking into websites which hold personal or financial information.

But even if you haven't fallen victim or don't think you are at risk, it's important to remember that online fraud can affect anyone, so it's vital to be alert.

Q Should online sites be doing more to protect our data?

A There have been recent high profile cases, where online sites have been targeted by fraudsters such as the Guardian jobs website and Spotify being hacked last year and personal information stolen, which obviously is very concerning. Legitimate websites are doing as much as they can to guard against fraud.

What we can advise is that consumers need to be aware of the risks of online fraud and need to protect themselves, monitor their statements and alert their bank to any transaction they think is fraudulent.

Q There have been lots of stories recently about social networking and privacy. How safe are social networking sites?

A Facebook has recently been criticised for making their privacy settings too complicated, meaning that many users are unsure what personal information is visible. But in the same way that you wouldn't hand out your personal information in the street, social network users should always assume that whatever information they have on their profile is in the public domain and can potentially be read by anyone, so should not put it up in the first place. The safety of social networking sites ultimately depends on the user themselves.

Q Is it a case of fraudsters just sending as many scams as possible in the hope that some people will fall victim?

A Quite possibly. It only takes a few people to fall victim to make it worthwhile for the fraudster, so as long as people keep falling victim, fraudsters will keep pushing their luck.

But it's not just a case of the quantity of scams. Fraudsters are investing in increasing how authentic they look. Some phishing e-mails are now so sophisticated that it's often very hard to tell a real e-mail from a fraudulent one.

Q **What advice are you giving people to protect themselves?**

A Consumers can reduce their chances of falling victim if they follow some basic precautions:

- They should never type credit card numbers, passwords, or any other confidential information into a web site unless its address begins with https and the browser displays the “closed padlock” symbol.
- Ensure that their antivirus software subscription is up to date, and that their computer is configured to automatically download and install any updates.
- They should never download attachments from untrusted sources.
- They should be wary of any e-mails or messages which ask for personal or financial data. Banks will never ask for personal information online.
- They should always check receipts against bank statements and contact their bank if concerned.
- They should check their bank statements regularly
- Register payment cards Verified by Visa or MasterCard SecureCode. It adds another layer to online security and makes it harder to fall victim to online fraud.
- On social networking sites, they should keep their privacy settings set to friends only and never display address, phone number or date of birth.
- Avoid carrying out transactions on public or shared computers.

If people are concerned, they can visit cpp.co.uk, which has some useful tips and an online test, which can tell them if they putting themselves at risk.

Q **How can you tell if you're a victim of online fraud?**

A One of the simplest ways you can find out you've been a victim of fraud is by spotting entries on your bank statement that you don't recognise. Other things to look out for include receiving welcome letters from credit card or loan companies that you've never contacted. You may receive calls from debt collection agencies chasing you for money that you never borrowed, or worryingly you may find that you are refused credit or have had important letters in the post that have gone missing. You may also find problems with your computer, if you have downloaded a virus or other malicious software.

We're urging all consumers to check their statements thoroughly and regularly themselves and to call the bank immediately if you suspect suspicious activity.

1.8 For further information please contact:

Nick Jones
Head of Communications
CPP Group Plc
Holgate Park
York YO26 4GA

Tel **01904 544 387**
E-Mail **nick.jones@cpp.co.uk**
Web **www.cppgroupplc.com**

CPP is an award-winning organisation:

- Finalist in the National Insurance Fraud Awards, Counter Fraud Initiative of the Year category, 2009
- Finalist in the European Contact Centre Awards, Large Team and Advisor of the Year categories, 2009
- Named in the Sunday Times 2008 PricewaterhouseCoopers Profit Track 100
- Finalists in the National Business Awards, 3i Growth Strategy category, 2008
- Finalist in the National Business Awards, Business of the Year category, 2007, 2009 and Highly Commended in 2008
- Named in the Sunday Times 2006, 2007, 2008 and 2009 HSBC Top Track 250 companies
- Regional winner of the National Training Awards, 2007
- Winner of the BITC Health, Work and Well-Being Award, 2007
- Highly Commended in the UK National Customer Service Awards, 2006
- Winner of the Tamworth Community Involvement Award, 2006. Finalist in 2008
- Highly Commended in The Press Best Link Between Business and Education, 2005 and 2006. Winner in 2007
- Finalist in the National Business Awards, Innovation category, 2005

1.9 About CPPGroup Plc

The CPPGroup Plc (CPP) is an international Life Assistance business offering bespoke management solutions to multi-sector business partners designed to enhance their customer revenue, engagement and loyalty, whilst at the same time reducing costs to deliver improved profitability.

This is underpinned by the delivery of a portfolio of complementary Life Assistance retail products, designed to help our mutual customers cope with the anxieties associated with the challenges and opportunities of everyday life.

Whether our customers have lost their wallets, been a victim of identity fraud or looking for lifestyle perks, CPP can help remove the hassle from their lives leaving them free to enjoy life. Globally, our Life Assistance products and services are designed to simplify the complexities of everyday living whether these affect personal finances, home, travel, personal data or future plans. When it really matters, Life Assistance enables people to live life and worry less.

Established in 1980, CPP has 10 million customers and more than 200 business partners across Europe, North and South America and Asia Pacific and employs 1,900 employees who handle millions of sales and service conversations each year.

In 2009, Group revenue was £292.1 million, an increase of more than 12 per cent over the previous year.

In March 2010, CPP debuted on the London Stock Exchange (LSE).

What We Do:

CPP provides a range of assistance products and services that allow our business partners to forge closer relationships with their customers.

We have a solution for many eventualities, including:

- Insuring our customers' mobile phones against loss, theft and damage
- Protecting the payment cards in our customers' wallets and purses, should these be lost or stolen
- Providing assistance and protection if a customer's keys are lost or stolen
- Providing advice, insurance and assistance to protect customers against the insidious crime of identity fraud
- Assisting customers with their travel needs be it an emergency (for example lost passport), or basic translation service
- Monitoring the credit status of our customers
- Provision of packaged services to business partners' customers

For more information on CPP visit:

www.cppgroupplc.com